25 ans du LIFO

Qualité de service et sécurité dans les réseaux de nouvelle génération

Francine Krief

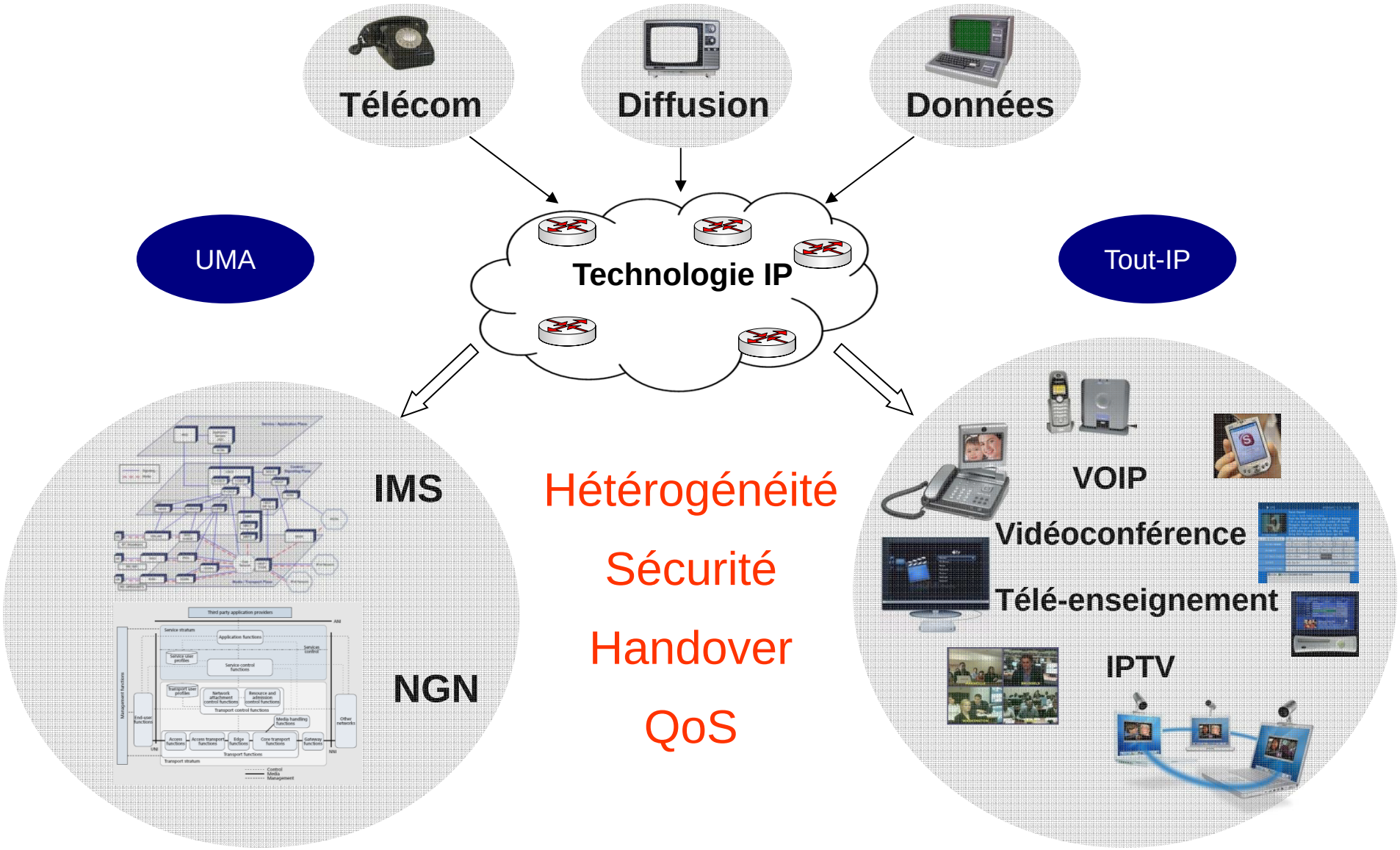
Université de Bordeaux
LaBRI
Équipe : LSR – Thème : COMET

Plan

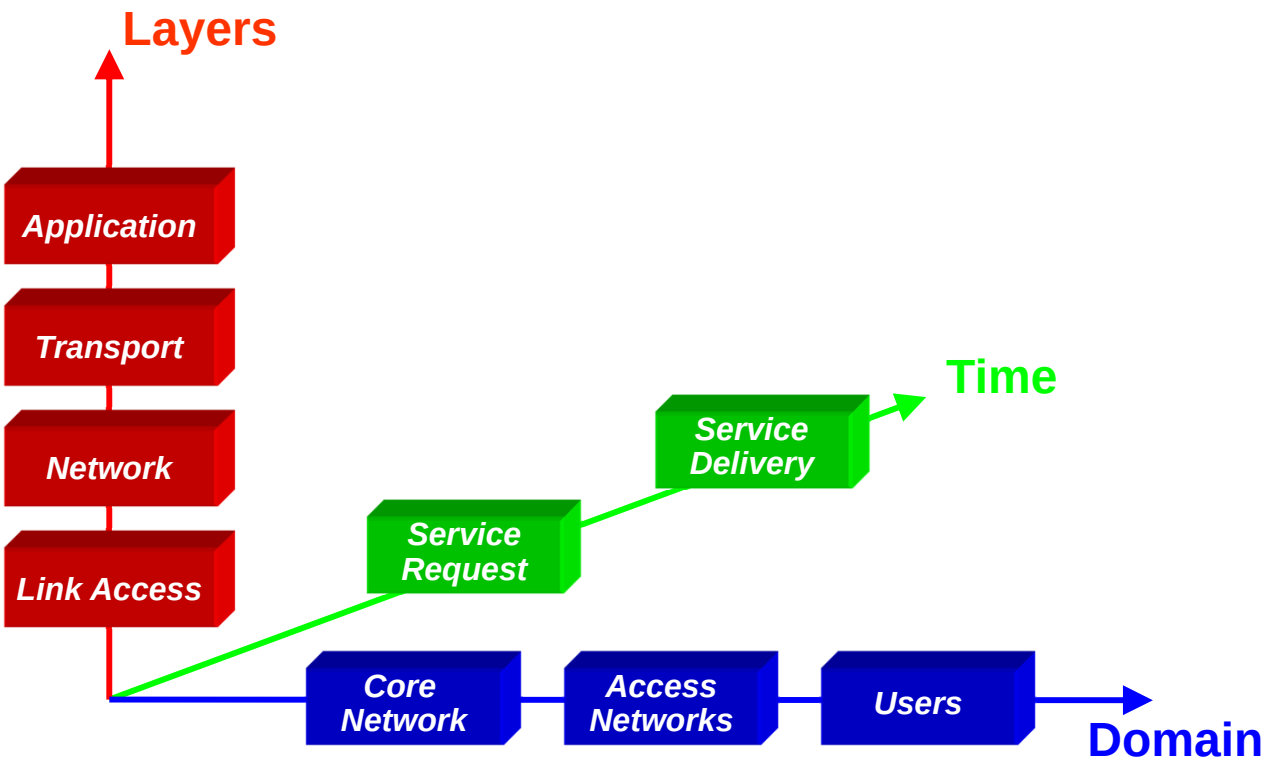
- ✓ **Introduction générale**
  - ✓ **Réseaux de nouvelle génération**
- QoS et Sécurité
- Economie d'énergie
- Autonomic networking
- Conclusion générale

Introduction générale

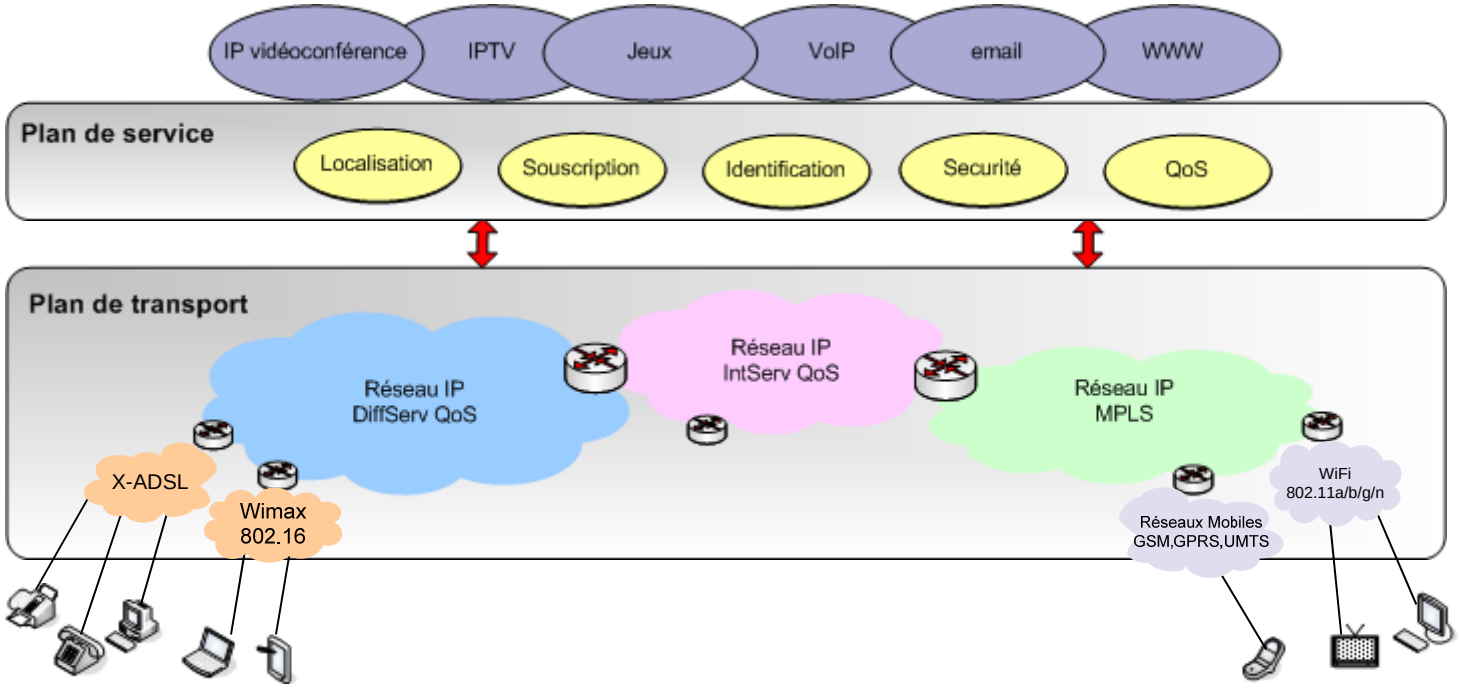
La convergence des réseaux et des services



La QoS dans les NGN



Les réseaux de nouvelle génération



QoS de bout en bout

Sécurité de bout en bout

Mobilité des utilisateurs

La qualité de service

- La QoS
  - Paramètres de performances associés à une connexion
  - Pallier aux problèmes inhérents à la technologie IP

- Les mécanismes de QoS
  - Dans les réseaux de transit : IntServ, DiffServ, MPLS/GMPLS, etc.
  - Dans les réseaux d'accès : Wi-Fi (802.11e), WiMax, etc.

- La QoS dans les NGN
  - Chaque domaine utilise son propre mécanisme pour gérer la QoS

  ⇨ Assurer une QoS homogène de bout en bout

La sécurité

- La sécurité
  - Services de sécurité : authentification, intégrité, confidentialité, etc.
  - Protéger contre les attaques menaçant la transmission de données

- Les mécanismes / protocoles de sécurité
  - Dans les réseaux de transit : IPSec, TLS, DTLS, etc.
  - Dans les réseaux d'accès : GSM, UMTS, Wi-Fi (WEP, WPA, WPA2), etc.

- La sécurité dans les NGN
  - Le réseau de cœur : aucune sécurité
  - Les réseaux d'accès : peu de sécurité

  ⇨ Assurer une sécurité de bout en bout

La mobilité

- La mobilité
  - Possibilité de changer de réseau d'accès
  - Pouvoir se connecter à tout moment et de n'importe où

- Les mécanismes / protocoles de mobilité
  - « Transport » : I-TCP, M-TCP, M-UDP, mSCTP, etc.
  - « Réseau » : MIP, MIPv6, etc.
  - « Liaison de données » : MIH (IEEE 802.21)

- La mobilité dans les NGN
  - Des réseaux d'accès très variés (technologie, débit, sécurité, etc.)
  - Cohabitation de ces réseaux dans une même zone
  - Assurer la mobilité d'un utilisateur ⟹ besoin incontournable

La négociation de niveau de service

- Un niveau de service
  - Défini par : un contrat SLA et des paramètres SLS
  - Couvre : la QoS, la sécurité et la mobilité

- Négociation de niveau de service
  - Assurer un niveau de service de bout en bout
  - Répondre aux besoins des utilisateurs (essentiellement la QoS)

- Protocoles de négociation de QoS
  - Extensions d'autres protocoles : RNAP (RSVP), COPS-SLS (COPS), etc.
  - Spécifiques à la négociation de SLS : DSNP, QoS-GSLP, SLNP, etc.

Qualité de Service et Sécurité

- La sécurité et la mobilité sont exclues de l'offre de service
- La sécurité et la mobilité peuvent avoir des incidences sur la QoS
- Impact de la sécurité sur la QoS ⇨ fausser l'offre de QoS
- Impact de la mobilité sur la QoS et la sécurité ⇨ changer les besoins

Besoin d'une offre de service globale

QoS, Sécurité et Mobilité

Plan

- ✓ Introduction générale
- ✓ **QoS et sécurité**
  - Etude de l'impact
  - Négociation conjointe
  - Négociation dans le NGN
- Economie d'énergie
- Autonomic networking
- Conclusion générale

QoS et Sécurité

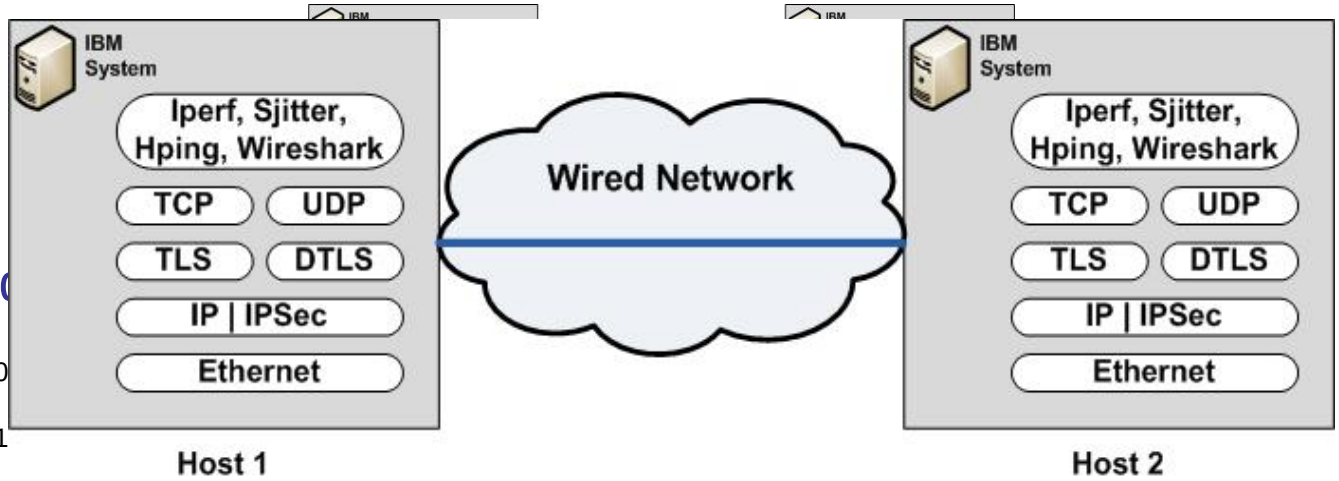
Plan

- ✓ Introduction générale
- QoS et Sécurité
  - Etude de l'impact
  - Négociation conjointe
  - Négociation dans le NGN
  - Sécurité de la négociation
- Economie d'énergie
- Autonomic networking
- Axes de recherche
- Conclusion générale

Etude et estimation de l'impact de la sécurité sur la QoS

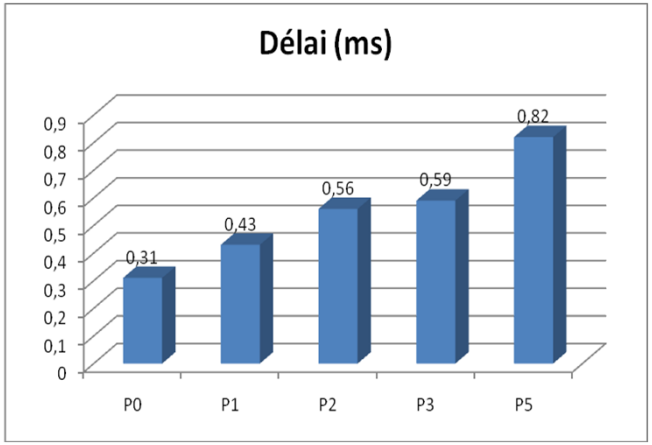
Mesures de l'impact

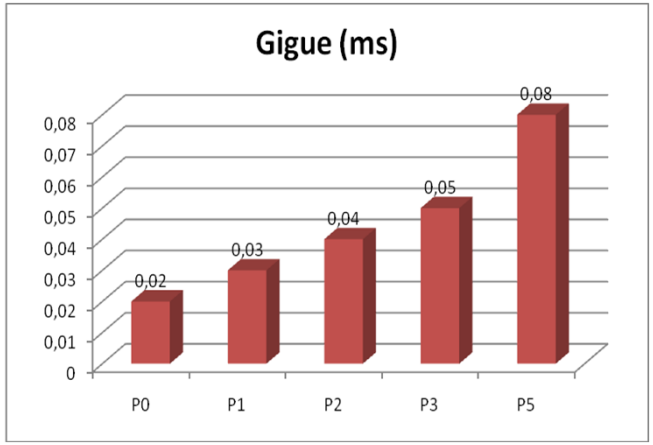
- Tests
  - Deux types de trafic : TCP et UDP
  - Paramètres de QoS mesurés : délai, gigue et bande passante
- Plateforme de tests



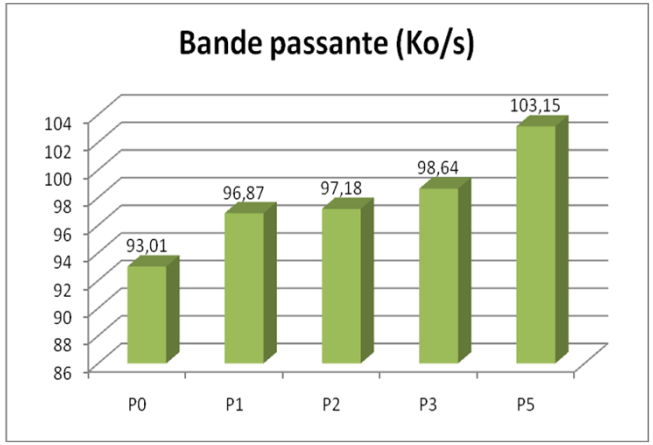
- Politi
  - P_0
  - P_1
  - P_2 : IPSec, ESP, Intégrité = hmac-sha1-96, Confidentialité = aes-cbc
  - P_3 : DTLS, Intégrité = sha1, Confidentialité = aes
  - P_4 : TLS, Intégrité = sha1, Confidentialité = aes
  - P_5 : $P_2 + P_3$
  - P_6 : $P_2 + P_4$

Résultats pour un trafic UDP



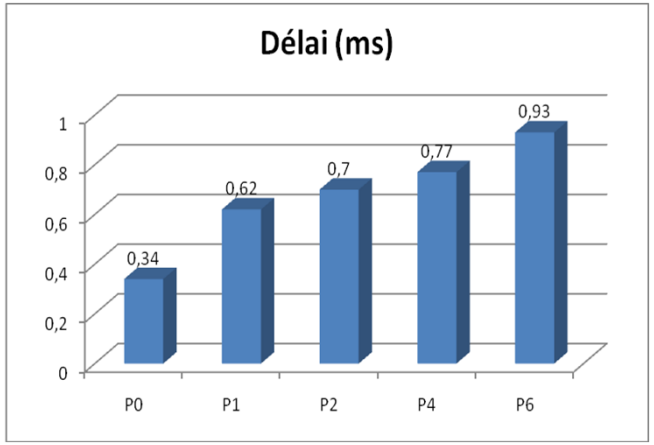


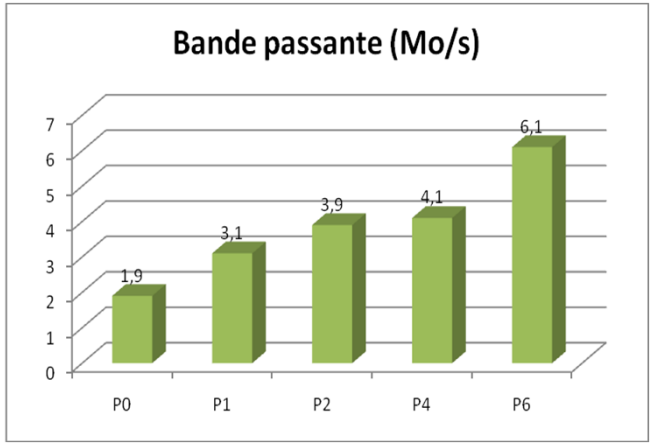
- L'ajout de la sécurité influence la QoS
- Impact (P_2) > Impact (P_1)
- Impact (P_2) ≃ Impact (P_3)
- Impact (P_5) ≃ Impact (P_2) + Impact (P_3)



Résultats pour un trafic TCP

- L'ajout de la sécurité influence la QoS
- Impact (P_2) > Impact (P_1)
- Impact (P_2) $\simeq$ Impact (P_4)
- Impact (P_6) $\simeq$ Impact (P_2) + Impact (P_4)



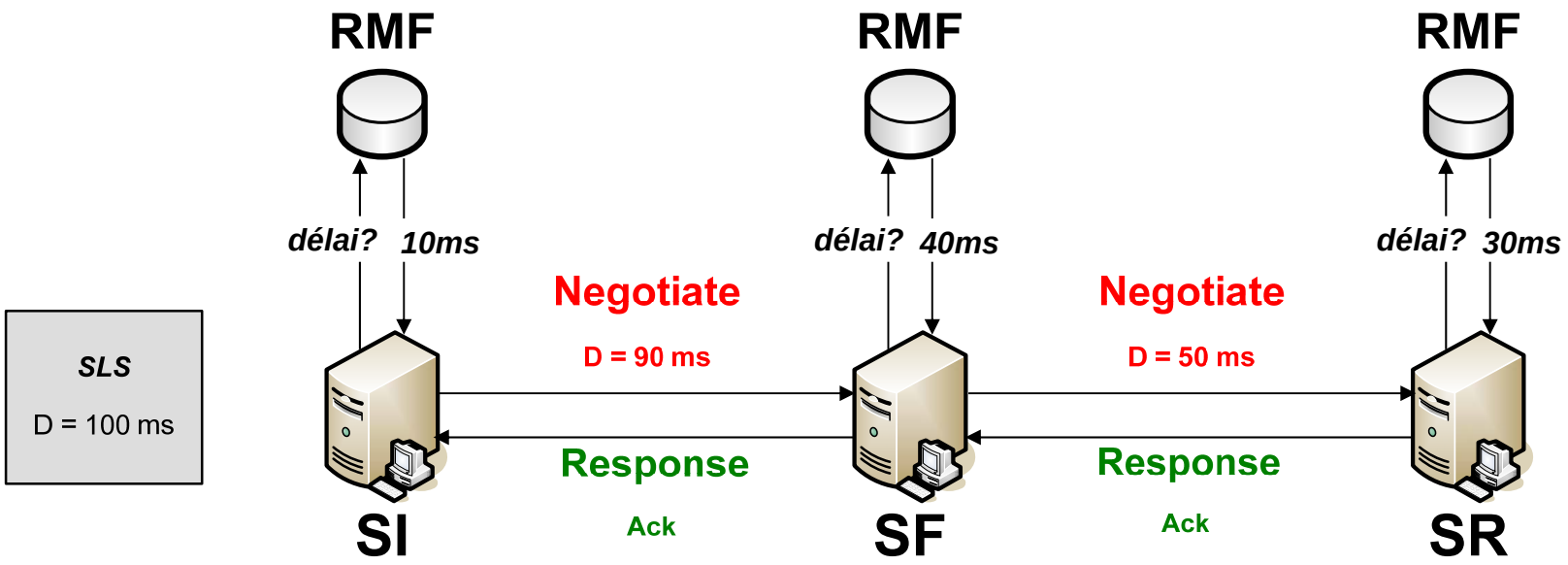


Plan

- ✓ Introduction générale
  - ✓ NGN
- QoS et Sécurité
  - ✓ Etude de l'impact
  - Négociation conjointe
  - Négociation dans le NGN
- Economie d'énergie
- Autonomic networking
- Conclusion générale

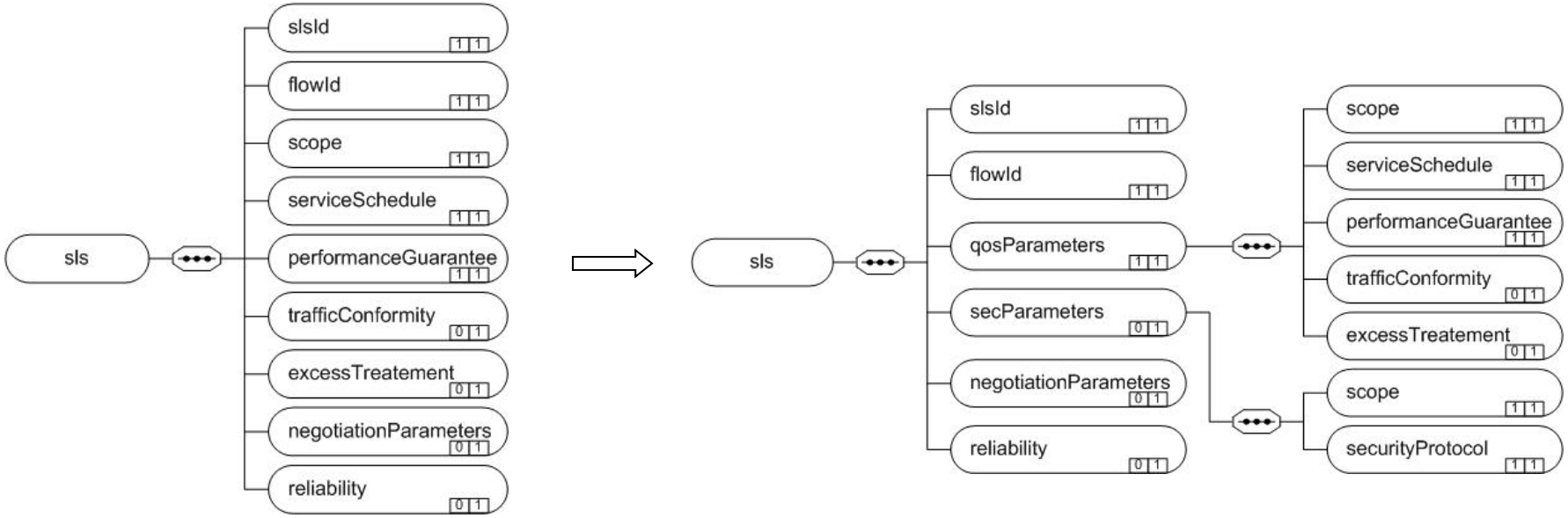
Négociation conjointe de la QoS et de la sécurité

Fonctionnement de la négociation de la QoS

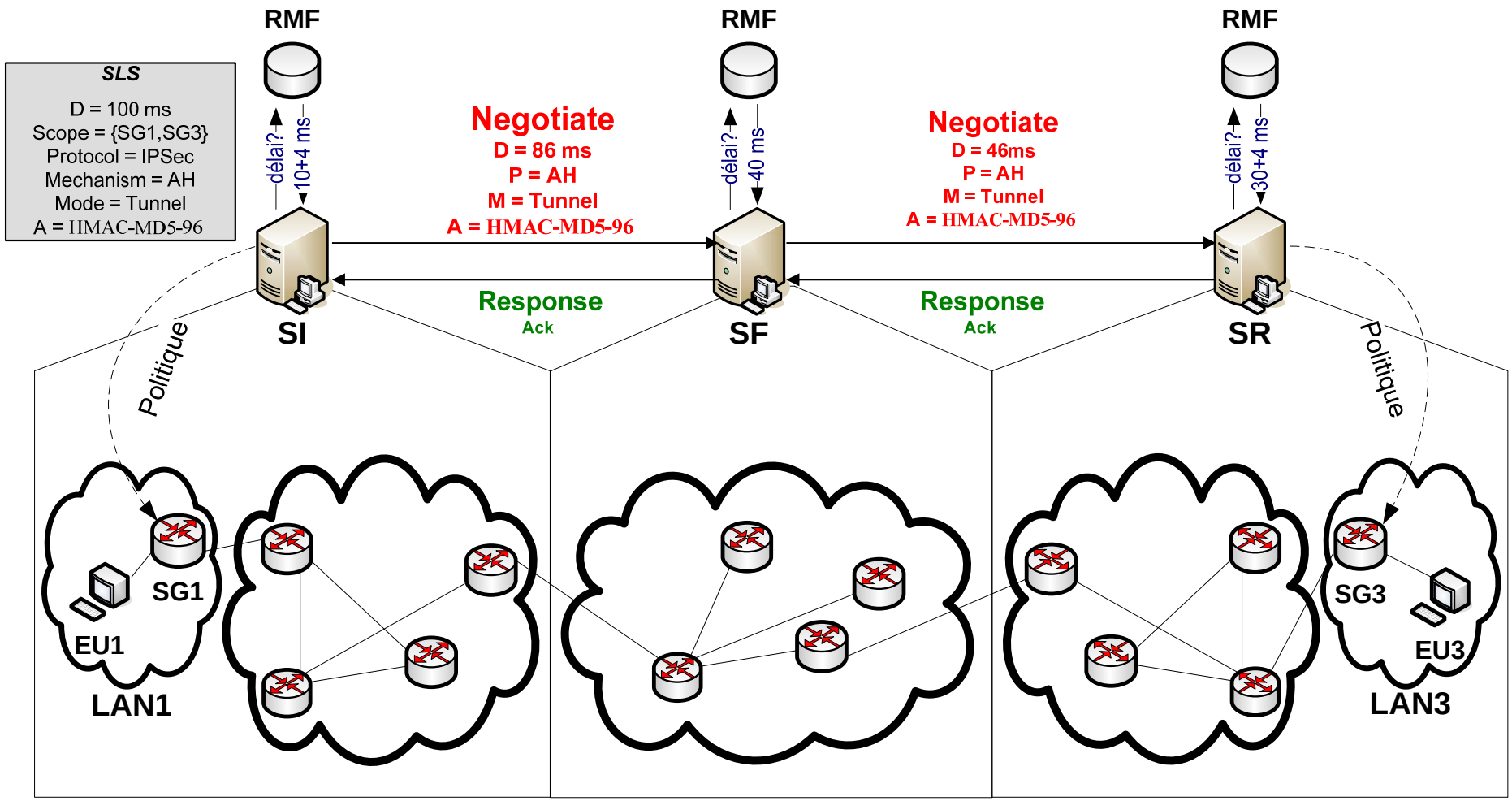


SLS de QoS et de sécurité

- Paramètres généraux : inchangeables
- Paramètres de QoS : regroupés dans l'élément 'qosParameters'
- Paramètres de sécurité : ajoutés et regroupés dans l'élément 'secParameters'
  - Portée de la sécurité
  - Protocole de sécurité à utiliser
  - Paramètres de sécurité relatifs au protocole sélectionné



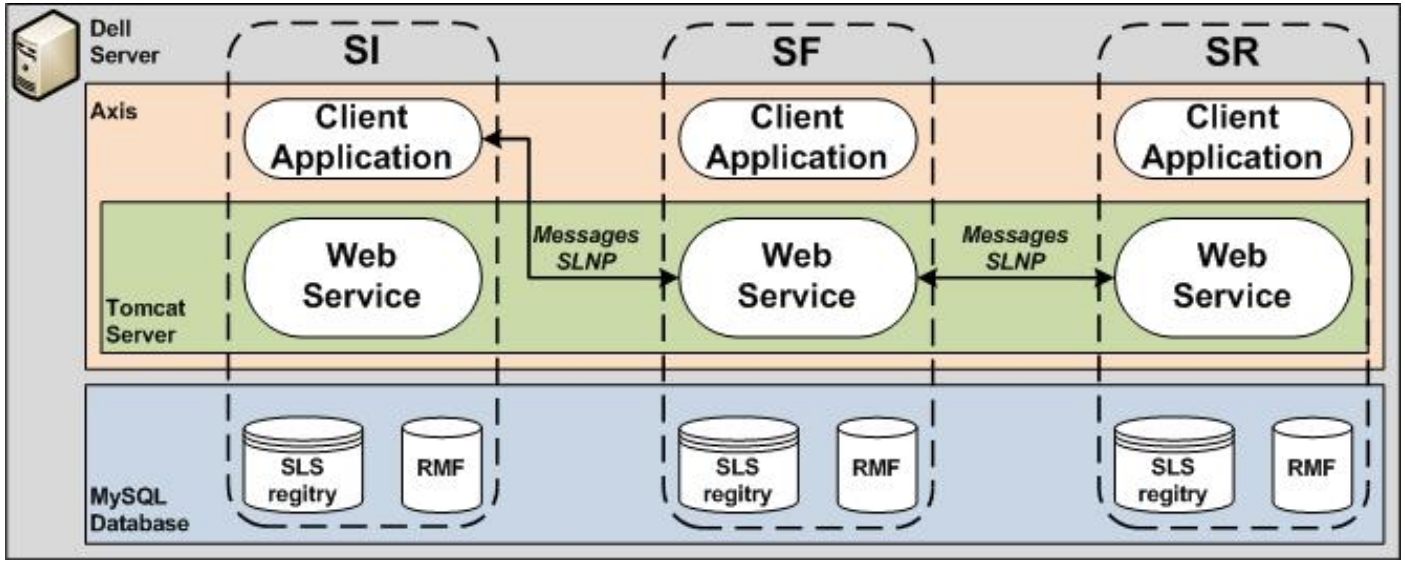
Fonctionnement de la négociation conjointe



Evaluation des performances de SLNP

- Tests
  - Performances : temps de négociation et taille de messages
  - Deux types de négociation : {QoS} vs {QoS + Sécurité}

- Plateforme de tests



Résultats des tests

- Temps de négociation

Type de négociation	Nombre total de scénarios	Nombre d'accords	Nombre moyen de passes	Temps moyen de négociation
QoS	10	8	1,7	114,13 ms
QoS + sécurité	50	22	4,48	307,50 ms

⇨ Accord sur la QoS et la sécurité plus difficile qu'un accord sur la QoS

- Temps d'une passe de négociation

Type de négociation	Temps moyen de négociation
QoS	60,08 ms
QoS + sécurité	62,61 ms

⇨ Augmentation légère (4,21 %) en introduisant la sécurité dans le SLS négocié

- Taille des messages

Type de négociation	Taille du message Negotiate
QoS	3749 octets
QoS + sécurité	4894 octets

⇨ Augmentation importante (30, 54 %) en introduisant la sécurité dans le SLS négocié

Plan

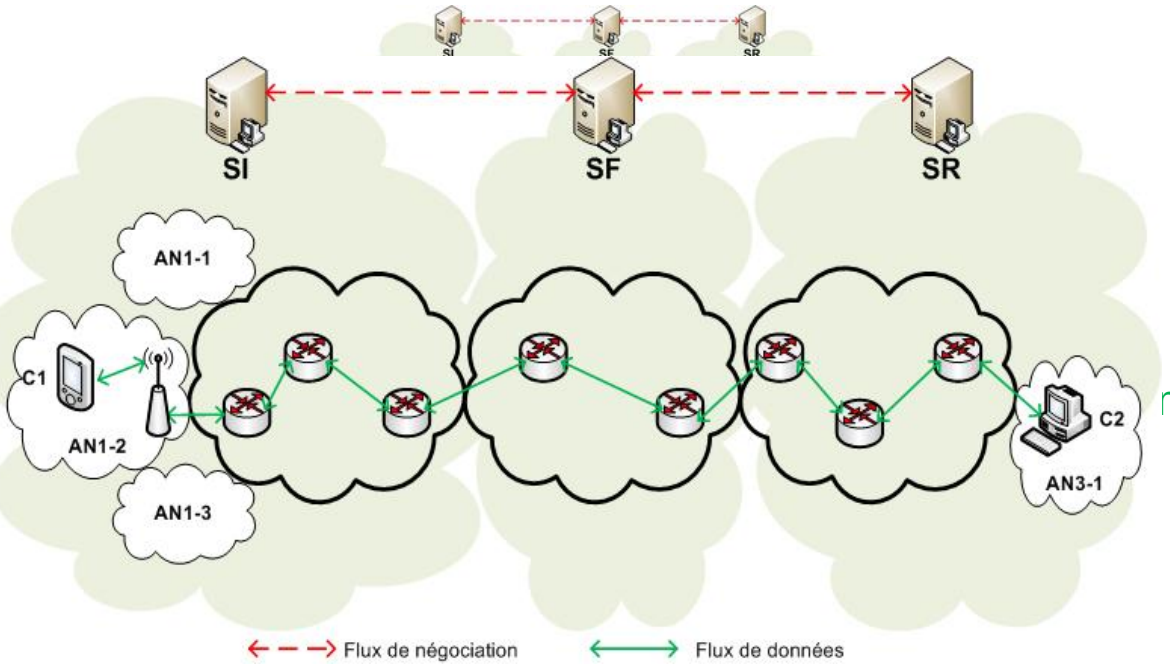
- ✓ Introduction générale
- QoS et Sécurité
  - ✓ Etude de l'impact
  - ✓ Négociation conjointe
  - Négociation dans le NGN
- Economie d'énergie
- Autonomic Networking
- Conclusion générale

Négociation dans les réseaux NGN

Motivation

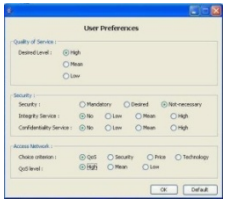
- Problème
  - Les réseaux NGN : multitude de réseaux d'accès et utilisateurs très mobiles
  - Les besoins des utilisateurs peuvent changer fréquemment ⟹ dynamicité

  ⇨ La négociation ne prend pas en compte la mobilité des utilisateurs

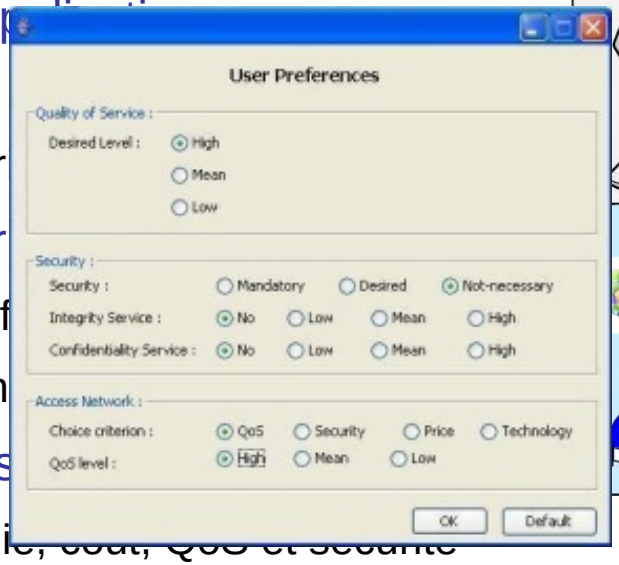


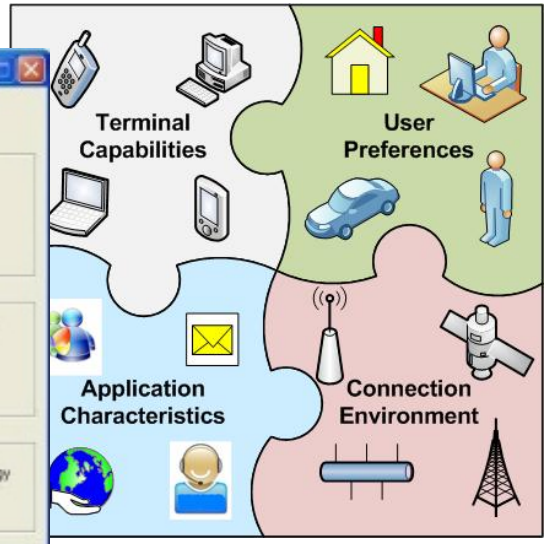
- Solution
  - Fonc matique du SLS
  - Gére
- Objectifs
  - Défir
  - Spécifier le fonctionnement de la négociation fondée sur le profil
  - Implémenter et évaluer les performances de la nouvelle version du protocole SLNP

Profil utilisateur pour la négociation



- Profil utilisateur
  - Stocker des informations sur l'environnement de la connexion
  - Quatre composantes : utilisateur, application, terminal et réseau d'accès
- Préférences de l'utilisateur
  - QoS : niveau souhaité (Bon, Moyen ou Minimal)
  - Sécurité : importance (facultative, souhaité ou obligatoire), services et niveaux
  - Réseau d'accès : critère de choix
- Caractéristiques de l'ap
  - Nom et type
  - Existence et caractér
- Caractéristiques du ter
  - Ecran, codecs et perf
  - Protocoles et algorith
- Caractéristiques du rés
  - Identifiant, technologie, coût, QoS et sécurité



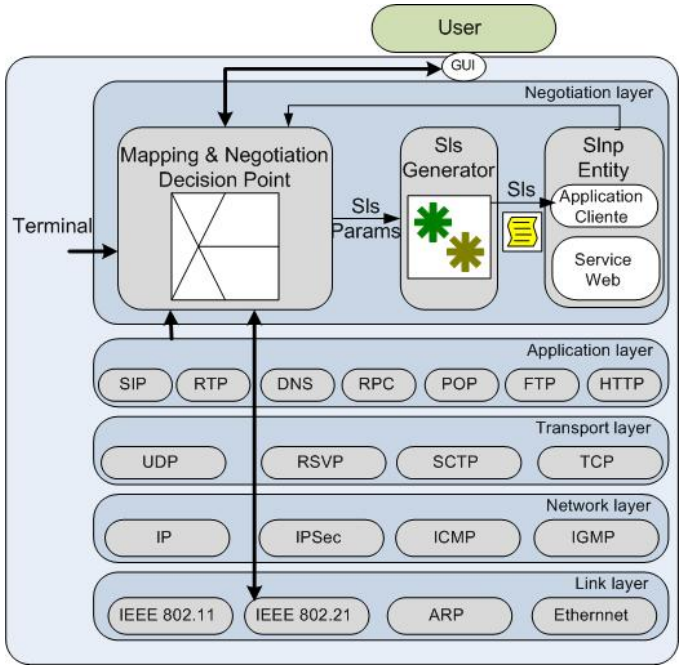


Négociation basée sur le profil

- Participation de l'utilisateur à la négociation
  - Négociation de SLS initiée par l'utilisateur
  - Définition du SLS requis sur la base du profil

  ⇨ Introduire une couche de négociation au niveau du terminal de l'utilisateur

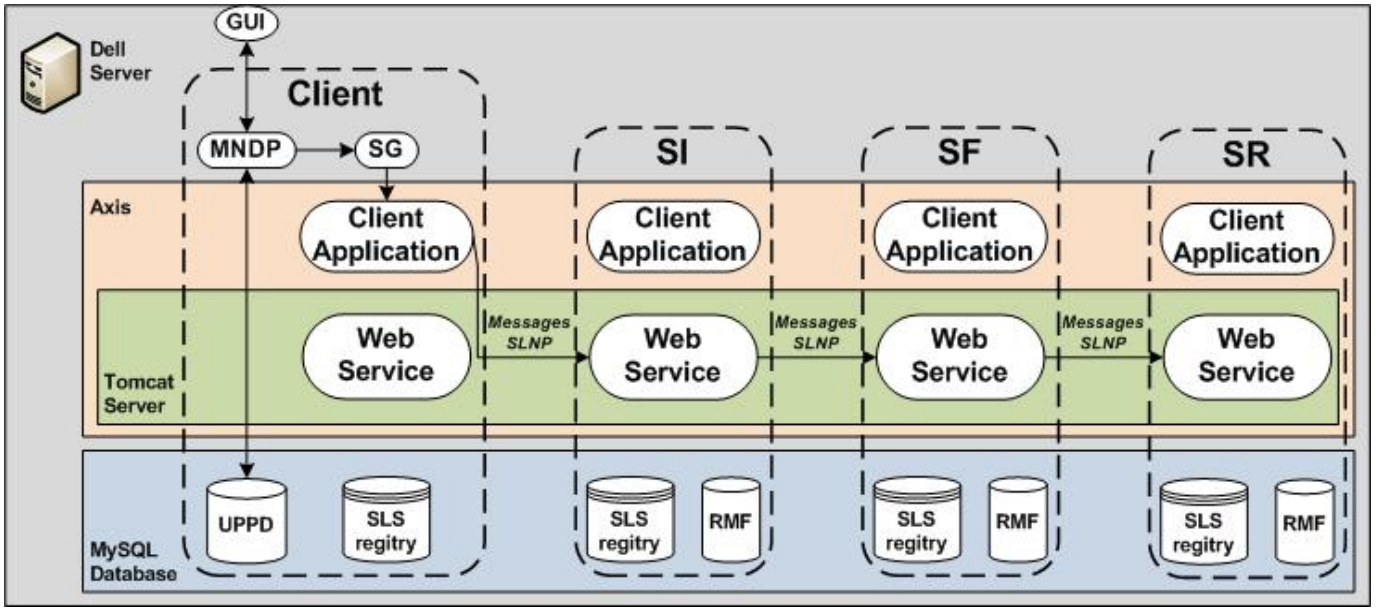
- Fonctionnement de la négociation
  1. Collecte ou mise à jour du profil
  2. Sélection d'un réseau d'accès
  3. Décision de négociation
  4. Définition des paramètres de SLS
  5. Génération de l'élément SLS
  6. Initiation de la négociation



Evaluation des nouvelles performances

- Tests
  - Performances : temps de négociation et taille de messages
  - Deux types de négociation : {classique} vs {adaptée aux NGN}

- Plateforme de tests



Résultats des tests

- Temps d'une passe de négociation

Type de négociation	Temps moyen de négociation
Classique	62,61 ms
NGN	97,42 ms

⇨ Augmentation de 55,6 % en impliquant l'utilisateur dans la négociation

- Taille des messages

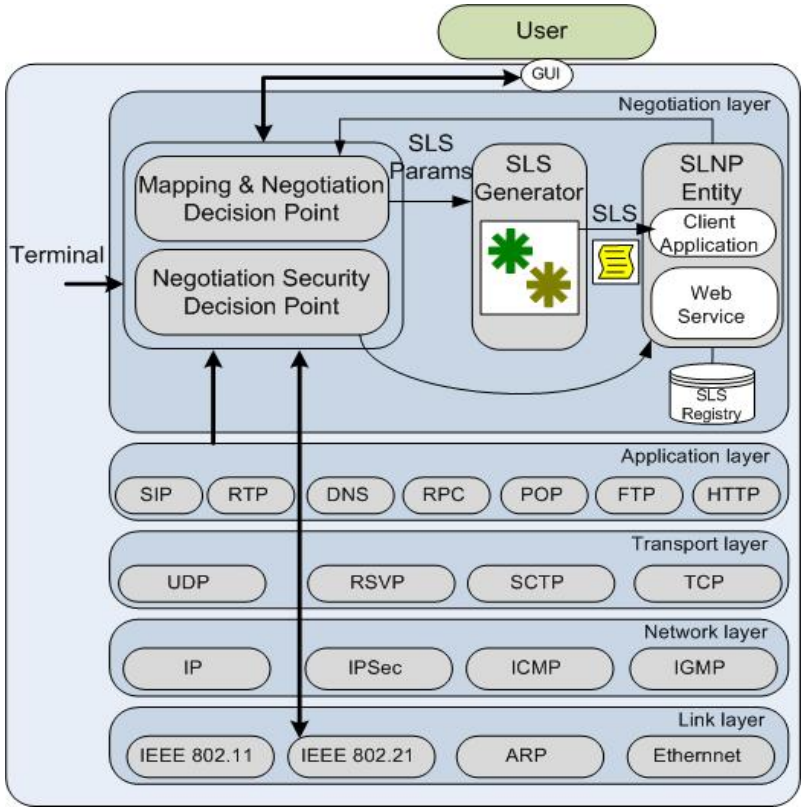
Type de négociation	Taille des messages
SI – SF – SR	4894 octets
Terminal – SI	4805 octets

⇨ Différence très légère entre les deux segments

Sécurisation du protocole SLNP

- Choix basé sur les performances de la négociation
  - Privilégier IPSec et SSL/TLS lorsqu'ils sont implémentés
  - Utiliser WSS lorsque IPSec et SSL/TLS sont indisponibles

- Modifications
  - Profil utilisateur – préférences
  - Composante NSDP



Plan

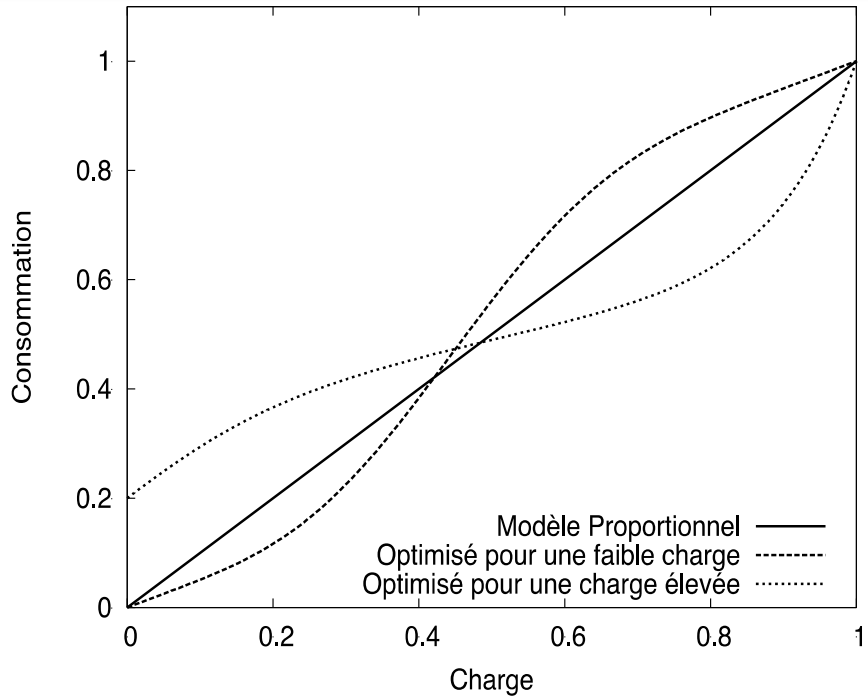
- ✓ Introduction générale
- QoS et Sécurité
- Economie d'énergie
  - ✓ Réseaux filaires
  - ✓ Réseaux mobiles
  - ✓ Réseaux sans fil
- Autonomic networking
- Conclusion générale

Economie d'énergie

Green Networking

- Réduire le volume d'émissions de gaz à effets de serre dues au processus de communication
  - TIC de plus en plus présents
    - 2 à 10 % des émissions de gaz à effets de serre
- Enjeux : Explorer les possibilités d'optimisation tout en limitant leur impact sur la QoS ou la tolérance aux pannes
- Difficultés à mesurer
  - Estimations contradictoires
    - RLE représentent 80% de la consommation énergétique de l'Internet
    - 50% attribué aux cartes d'interface
    - Réseaux cœur équivalent aux réseaux d'accès en 2017

Modèles de consommation énergétique



- La définition d'une politique globale au niveau d'un ensemble de ressources constitue un problème d'optimisation non trivial
- Autres enjeux
  - Caractérisation des profils de consommation
  - Critères d'évaluation de base

Green Networking – Réseaux filaires

- Actions possibles à plusieurs niveaux
  - Phase de planification d'un réseau de communication
  - Phase de fonctionnement
- Applications et protocoles de transport
  - Optimiser le comportement des applications (Ex : Green BitTorrent)
  - Protocole TCP (EX : TCP_SLEEP)
  - Virtualisation, migration de services
  - Liens de communication
    - Mise en veille de certains liens tout en préservant la QoS
    - stratégie d'adaptation des débits
  - Agrégation des flux pour le routage

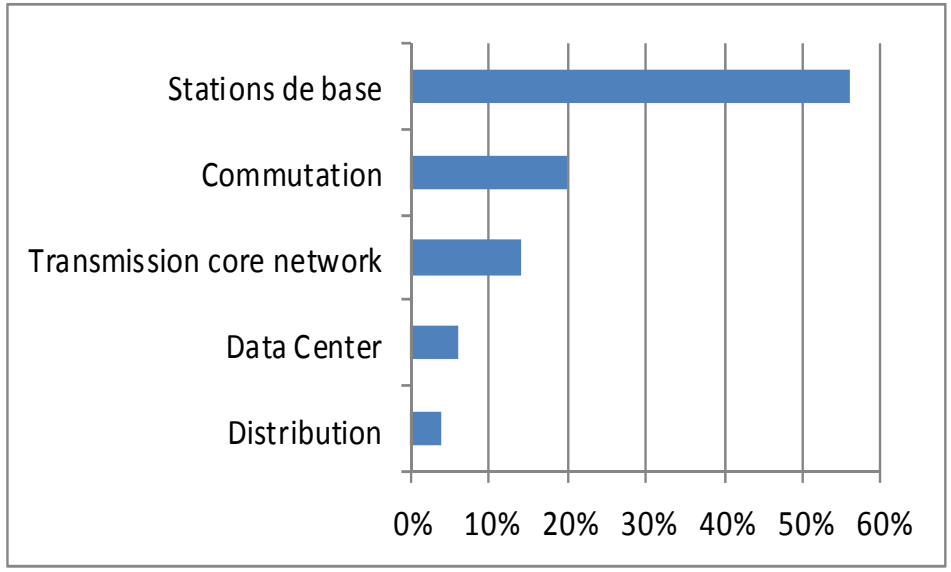
Plan

- ✓ Introduction générale
- QoS et Sécurité
- Economie d'énergie
  - ✓ Réseaux filaires
  - ✓ Réseaux mobiles
  - ✓ Réseaux sans fil
- Autonomic networking
- Conclusion générale

Economie d'énergie dans les réseaux mobiles

Green Networking – Réseaux mobiles

- Réseaux cellulaires = systèmes limités par les interférences
- Consommation d'énergie particulièrement importante dans la partie communication
  - Réseau d'accès radio = 57% de l'électricité consommée



Distribution de la consommation de puissance pour un opérateur de réseau cellulaire

Green Networking – Réseaux mobiles

- Processus et protocoles
  - Nombreuses techniques élaborées et intégrées aux normes
    - DTX (Discontinuous Transmission), DRX (Discontinuous Reception) ou sleep dans les réseaux WiMAX
  - Planification dynamique
    - Adaptation de l'activité du réseau au trafic
  - Agrégation du trafic en fonction du délai
    - Compromis à trouver car impacte la QoS
  - Coopération entre stations de base
  - Association MS-BTS
    - Mécanisme de handover

Green Networking – Réseaux mobiles

- Architectures réseaux
  - Relaying et multi-hoping
    - Réduction de puissance
  - Micro-cellules
    - Réduction du rayon d'une cellule -> réduction consommation de puissance
  - Evolution vers le tout-IP et les architectures plates
    - Couche unique de stations de base reliées entre elles par des liens haut débit
  - Antennes intelligentes
    - Réduction des rayonnements

Plan

- ✓ Introduction générale
- QoS et Sécurité
- **Economie d'énergie**
  - ✓ Réseaux filaires
  - ✓ Réseaux mobiles
  - ✓ **Réseaux sans fil**
- Autonomic networking
- Conclusion générale

Economie d'énergie dans les réseaux sans fil

Green Networking – Réseaux sans fil

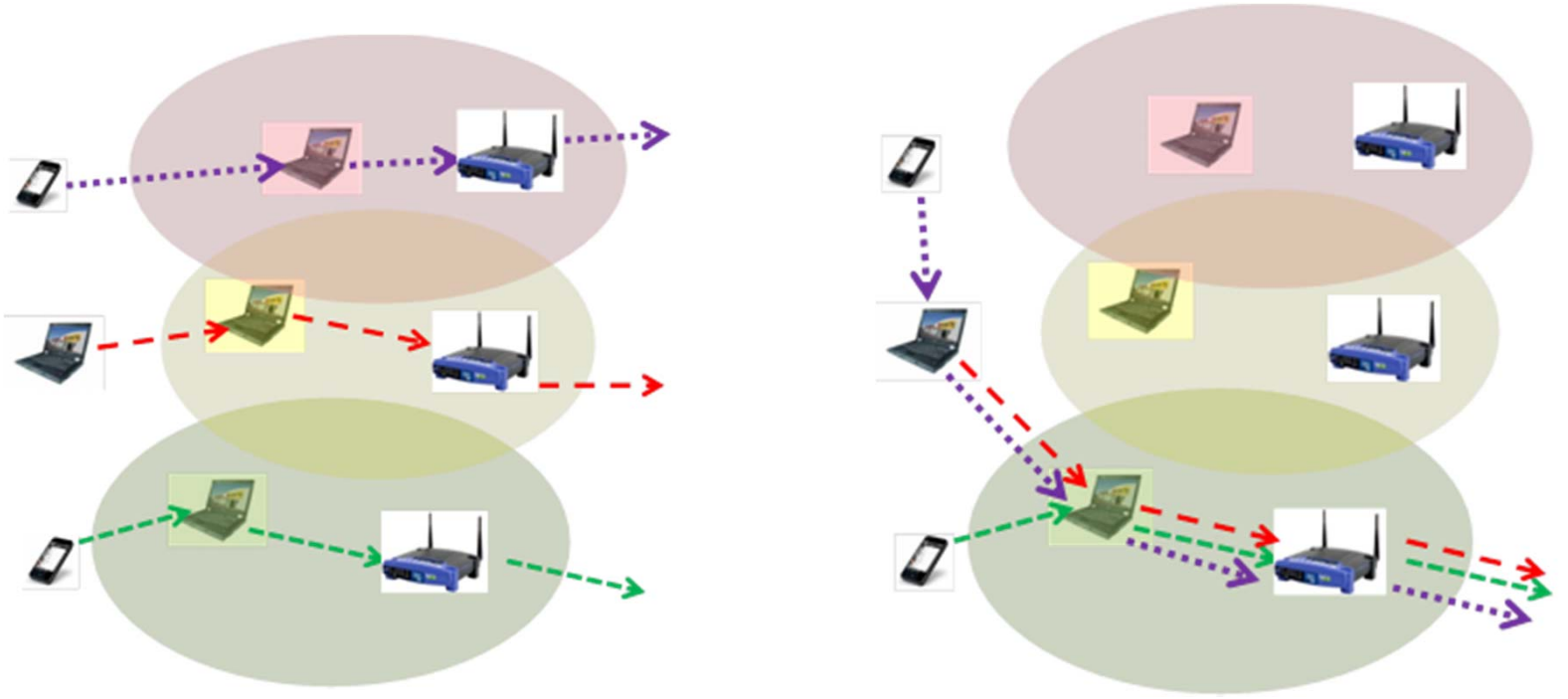
- Les réseaux d'accès sont un des points importants dans la consommation énergétique.

- Points d'accès
  - Les points d'accès d'aujourd'hui consomment souvent bien plus de 10 W
  - Il est à noter que les points d'accès IEEE 802.11n et encore plus la nouvelle génération IEEE 802.11ac puis af consomment nettement plus d'énergie, de 20 à 50 W

- Terminaux
  - PC portables ont souvent des émissions WiFi de l'ordre d'une trentaine de mW

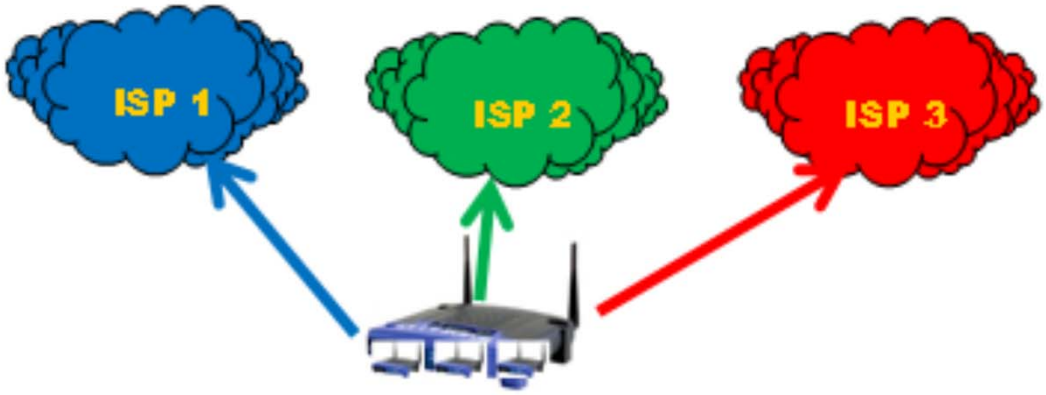
Green Networking – Réseaux sans fil

- Les réseaux « low cost » et économe en énergie



Green Networking – Réseaux sans fil

- Avantage de la virtualisation
  - Il est possible de rassembler sur une même machine physique un grand nombre de machines virtuelles jusqu'à utiliser au mieux la machine physique.
  - Si l'équipement physique est très puissant, on peut y mettre de nombreuses machines virtuelles qui peuvent s'éteindre et s'allumer sans problème. On peut y charger de nouvelles machines virtuelles comme en décharger d'autres.
  - Le gain en économie d'énergie provient en grande partie du partage qui peut être réalisé d'une infrastructure physique commune.

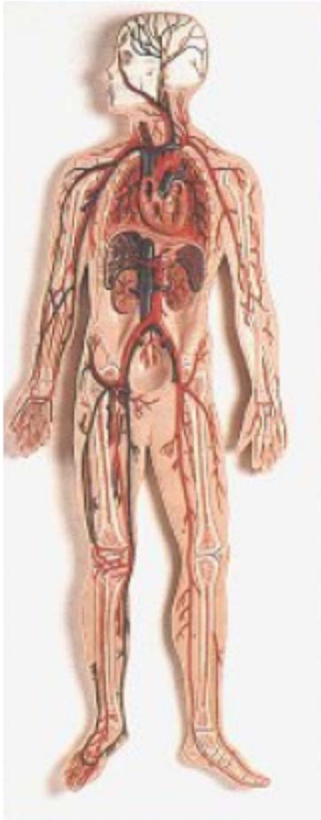


Plan

- ✓ Introduction générale
- QoS et Sécurité
- Economie d'énergie
- ✓ Autonomic networking
  - ✓ Concepts
  - ✓ Exemples
- Conclusion générale

Autonomic networking

Vision de l'autonomie



- Le système nerveux autonome : une source d'inspiration (battement du cœur, régulation de la respiration...).
  - Lancement en 2001 de l'initiative Autonomic Computing par IBM
- Construire un système fiable sur lequel nous pouvons compter (survie, disponibilité, sûreté, sécurité...).
  - Une approche holistique : Rassembler et harmoniser tous les domaines de recherche qui peuvent contribuer à la réalisation des réseaux autonomes

- La vision de l'autonomie : création d'un système qui sait s'autogérer (*Self Management System*)

Objectifs de la gestion autonome

- Temps de Réponse Amélioré
  - Adaptation dynamique aux changements de l'environnement

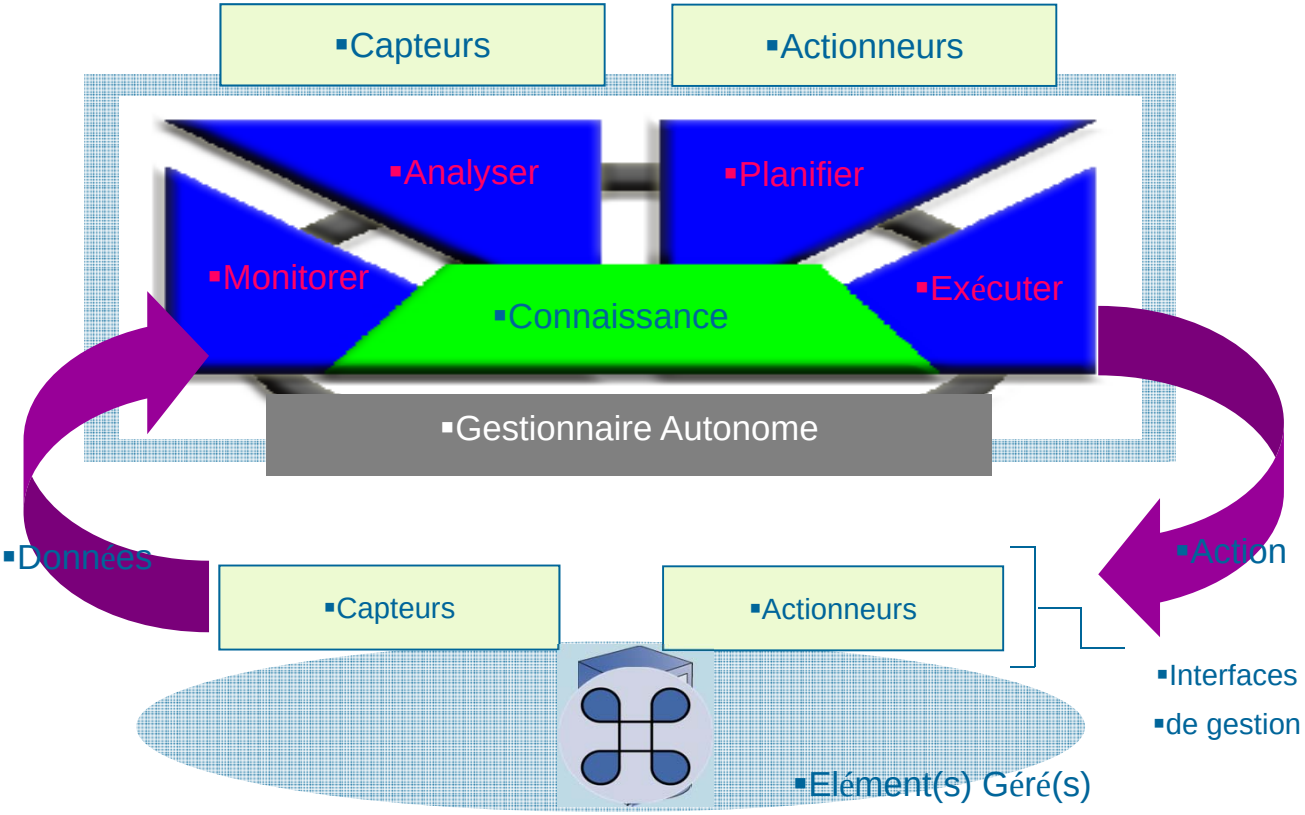
- Plus de Stabilité
  - Découvrir, diagnostiquer, et agir pour éviter des pannes

- Efficacité Opérationnelle
  - Ajuster les paramètres de performance et permettre une meilleure utilisation des ressources

- Des Ressources Sécurisées
  - Anticiper, détecter, identifier, et se protéger contre les attaques

Quatre fonctions principales

Architecture d'une entité autonome

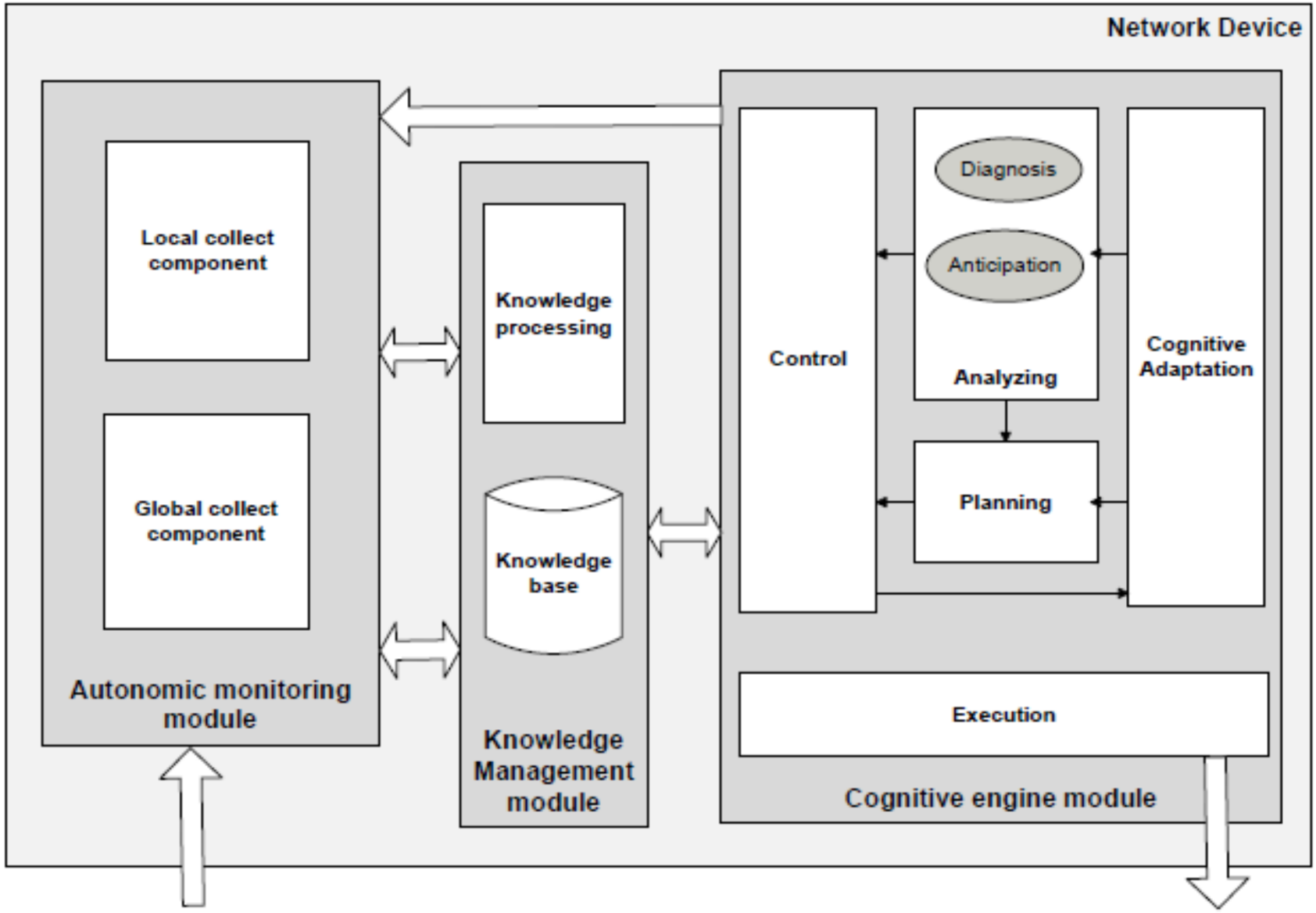


Plan

- ✓ Introduction générale
- QoS et Sécurité
- Economie d'énergie
- ✓ Autonomic networking
  - ✓ Concepts
  - ✓ Exemples
- Conclusion générale

Exemples d'architectures autonomes

Architecture SADA



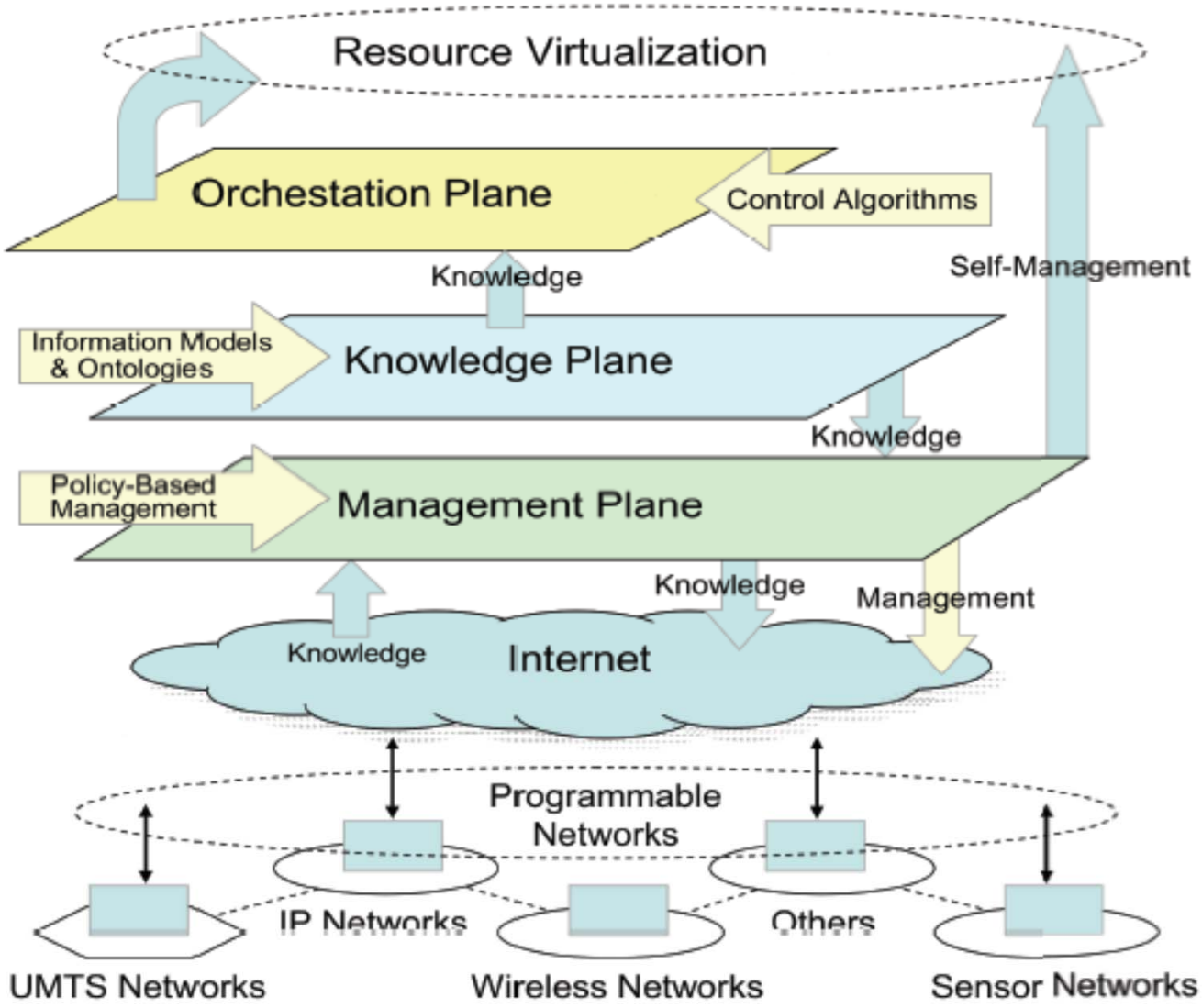
Architecture SADA

- SRS (Self-adaptive Routing Scheme)
  - Auto-adaptation processus de découverte de routes dans le cadre des protocoles de routage des réseaux MANET
  - Mécanisme d'apprentissage par renforcement utilisé pour privilégier ou éviter certains chemins en se basant sur leur performance passée
- ATMS (Autonomic Trust Knowledge Monitoring Scheme)
  - Collecte information locale et globale nécessaire à l'établissement des relations de confiance entre paires de nœuds dans un réseau MANET autonome

[1] Z. Movahedi, M. Nogueira, G. Pujolle, An Autonomic Knowledge Monitoring Scheme for Trust Management on Mobile Ad Hoc Networks, Wireless Communications and Networking Conference (WCNC 2012), September 2011

[2] G. Bella, G. Costantino, and S. Riccobene, «Managing reputation over manets», in Proceedings of the Fourth International Conference on Information Assurance and Security, (Washington, DC, USA), pp. 255{260, IEEE Computer Society, 2008.

Architecture AUTo I



Plan

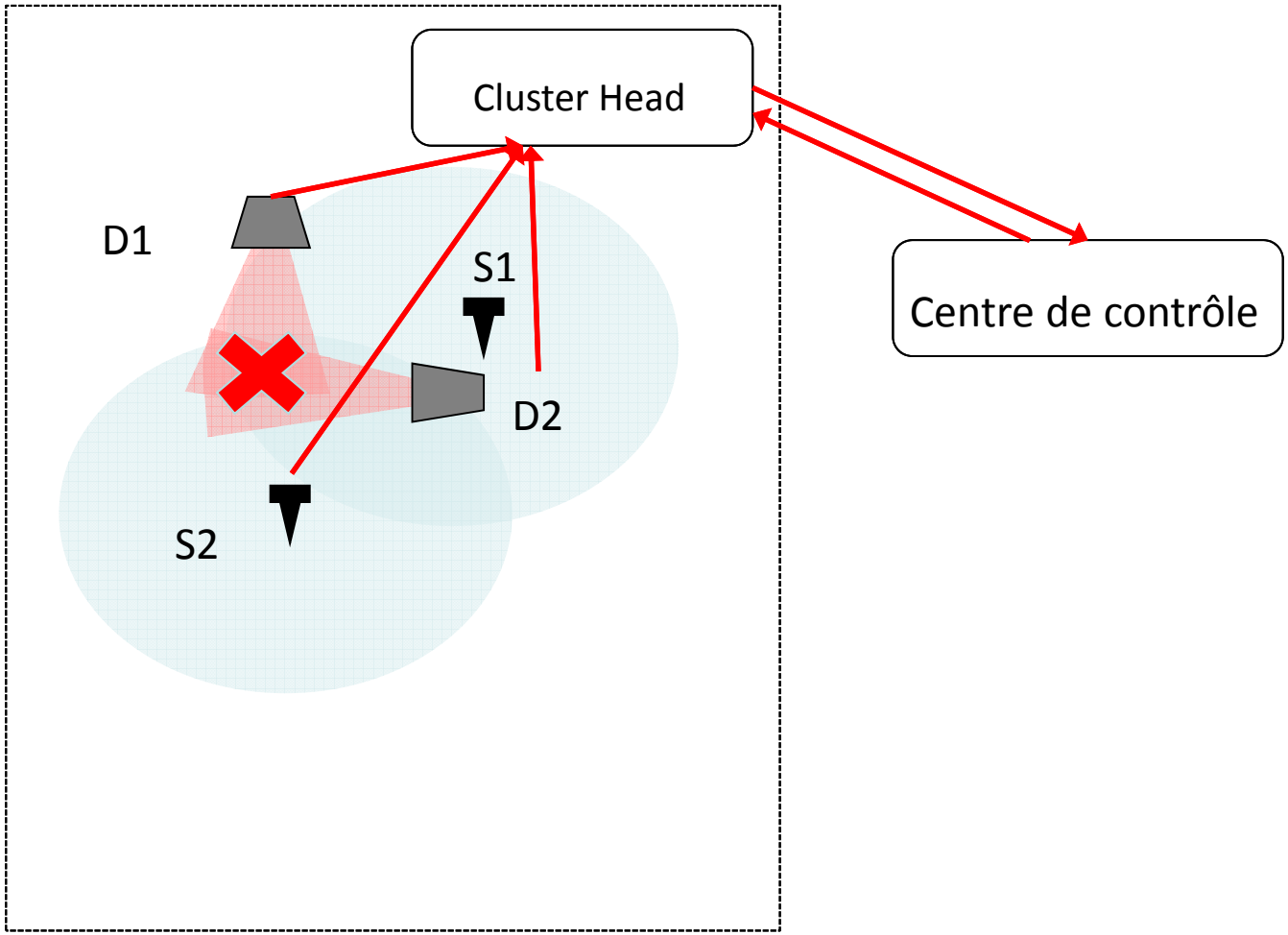
- ✓ Introduction générale
- QoS et Sécurité
- Economie d'énergie
- Autonomic networking
- Conclusion générale
- ✓ **Autres axes de recherche**

Conclusion générale

Approches collaboratives

- Exemple dans un réseau de capteurs sans fil

Gestion de la réputation

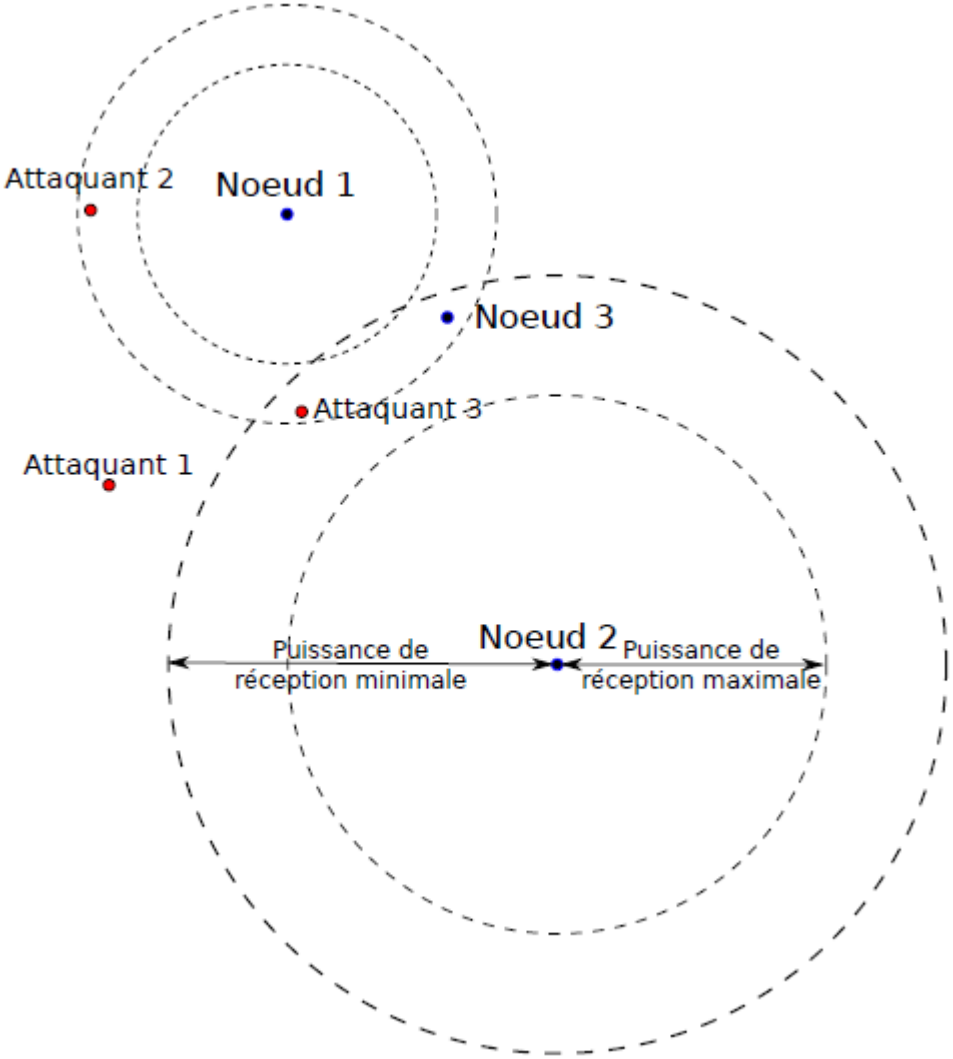


Approches collaboratives

- Exemple dans un réseau de capteurs sans fil

Triangulation distribuée

Les attaquants 1, 2 et 3 essaient de se faire passer pour le nœud 3



Défis scientifiques

- La sécurité, la confiance et le respect de la vie privée
  - Conception de systèmes communicants garantissant la sécurité des usagers et des données, développer des services assurant aux auteurs/usagers la maîtrise du cycle de vie des données injectées sur le réseau (support de l'oubli numérique); modèles de confiance et protocoles associés pour développer différentes fonctions du réseau, cryptographie, notamment cryptographie quantique.

- La mobilité généralisée des services
  - Architectures fonctionnelles et protocolaires pour la continuité des services ainsi que de la qualité de service et d'expérience, Réseaux tolérants aux pannes et aux délais (DTNs), Modélisation de la mobilité, modélisation des contacts, Extraction de paramètres pour la conception et optimisation de protocoles, Optimisation multicouches et multi-accès.

Défis scientifiques

- L'explosion du nombre d'objets qui seront mis en réseaux
  - **Auto-organisation** dans des systèmes intelligents capables d'acquérir et de traiter localement des informations, de prendre des décisions et d'agir sur leur environnement

- La ville intelligente, le maintien a domicile, la surveillance, etc.
  - **Auto-organisation** sensible aux applications et au trafic, capture, agrégation et traitement décentralisé, notamment dans le réseau, des données captées, transport en contexte de mobilité de trafics avec des contraintes spécifiques, **auto-adaptation et auto déploiement** des infrastructures en fonction des évolutions applicatives, description sémantique décentralisée des données.

- La fiabilité de systèmes sur lesquels reposera notamment la santé des individus et le maintien de l'environnement.

Merci pour votre attention